



M5249RDUG
5/2003
REV 2

MCF5249 Fingerprint Security Reference Design User's Guide

Freescale Semiconductor, Inc.

HOW TO REACH US:

USA/EUROPE/LOCATIONS NOT LISTED:

Motorola Literature Distribution
P.O. Box 5405, Denver, Colorado 80217
1-303-675-2140 or 1-800-441-2447

JAPAN:

Motorola Japan Ltd.
SPS, Technical Information Center
3-20-1, Minami-Azabu Minato-ku
Tokyo 106-8573 Japan
81-3-3440-3569

ASIA/PACIFIC:

Motorola Semiconductors H.K. Ltd.
Silicon Harbour Centre, 2 Dai King Street
Tai Po Industrial Estate, Tai Po, N.T., Hong Kong
852-26668334

TECHNICAL INFORMATION CENTER:

1-800-521-6274

HOME PAGE:

<http://www.motorola.com/semiconductors>

DOCUMENT COMMENTS:

FAX (512) 933-2625
Attn: TECD Applications Engineering

Information in this document is provided solely to enable system and software implementers to use Motorola products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits or integrated circuits based on the information in this document.

Motorola reserves the right to make changes without further notice to any products herein.

Motorola makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Motorola assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. "Typical" parameters which may be provided in Motorola data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including "Typicals" must be validated for each customer application by customer's technical experts. Motorola does not convey any license under its patent rights nor the rights of others. Motorola products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the Motorola product could create a situation where personal injury or death may occur. Should Buyer purchase or use Motorola products for any such unintended or unauthorized application, Buyer shall indemnify and hold Motorola and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Motorola was negligent regarding the design or manufacture of the part.



Motorola and the Stylized M Logo are registered in the U.S. Patent and Trademark Office. digital dna is a trademark of Motorola, Inc. All other product or service names are the property of their respective owners. Motorola, Inc. is an Equal Opportunity/Affirmative Action Employer.

© Motorola, Inc. 2003

**For More Information On This Product,
Go to: www.freescale.com**

About This Document

The primary objective of this document is to provide a quick introduction to the MCF5249 Fingerprint Biometrics Reference design.

Audience

This document is intended for users of the reference design hardware and software, that is, the M5249C3 Biometrics daughter card and the executable software.

Suggested Reading

The following documents provide background for the information in this user's guide.

- *Integrating the MCF5249 to a Biometric Fingerprint Sensor (AN2382/D)*
- *MCF5249 ColdFire Integrated Microprocessor User's Manual, R0.1 (MCF5249UM/D)*
- *M5249C3 User's Manual, R1.1 (M5249C3UM/AD)*

Requirements

This document assumes that the reader is in possession of the following:

- M5249C3 evaluation board (EVB) with dBUG version v3a.1b.1b (Sep 26 2002) or later (Previous versions may have problems with ethernet download. See the ColdFire website, www.motorola.com/ColdFire, for dBUG upgrades if required.)
- M5249C3 Biometrics Security daughter card
- RS232 cable
- Ethernet cable (crossed if not connecting through a network)
- tftp server running on the PC (available from the NetBurner website, www.netburner.com)
- Flash programmer (CFFlasher.exe is available from the Motorola website, e-www.motorola.com/collateral/CFFLASHER.htm)

This document also assumes that the reader has read AN2382/D, *Integrating the MCF5249 to a Biometric Fingerprint Sensor*, and has downloaded the demonstration biometric application containing the Acter AG biometric algorithm from the ColdFire website.

1 Introduction

This document describes how to set up and run the demonstration biometric application which functions as a simple fingerprint recognition system. It details how to download the application to the M5249C3 EVB, how to run it, and how to interact with it.

1.1 Key Features

The MCF5249 Biometrics Security Reference Design is comprised of a daughter card designed to fit onto the M5249C3 EVB and EVB application software. The daughter card includes a user interface in the form of an LCD panel and a fingerprint sensor as shown in Figure 1.

NOTE

If the application has been programmed into the EVB Flash, fitting the daughter card to the EVB and connecting the power supply causes the application to run automatically.

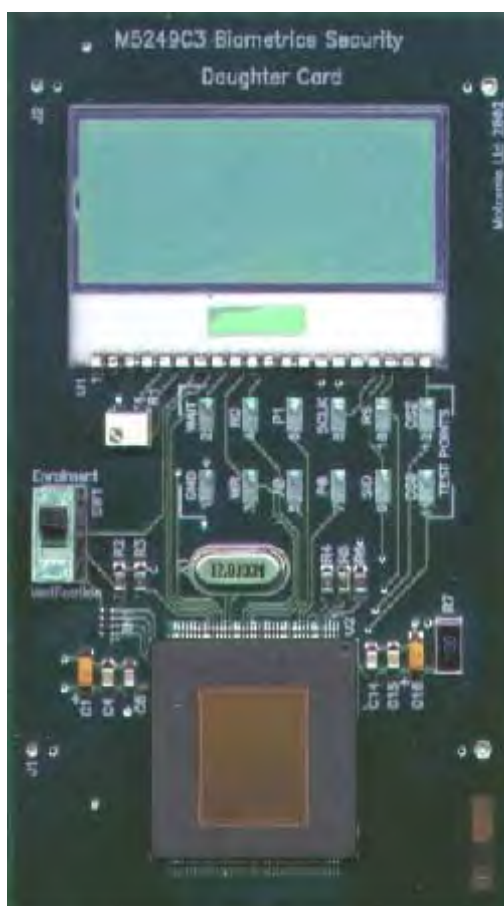


Figure 1. M5249C3 Biometrics Security Daughter Card

2 Setup

Carefully follow these steps to set up the biometrics fingerprint reference design for demonstration.

2.1 Flash Version

1. Fit the Biometrics Security daughter card to the M5249C3 EVB using the expansion connectors. The connectors are keyed and will only fit one way, with the sensor on the IDE connector side of the EVB and the LCD on the BDM connector side.
2. Connect the P&E wiggler and power cables to the EVB.
3. Run CFFlasher.exe, click on Target Configuration, and select the MCF5249C3 radio button.
4. Click on Program Flash, browse for the MCF5249BIOflash.s19 S-record, and click on Program. The S-record will be programmed starting at address 0XFFF00000.
5. Disconnect the power and P&E wiggler and switch jumper 12 from pins 1–2 to pins 2–3 on the EVB and reconnect the power cable. Jumper 12 determines where in Flash the board will boot from (See section 3.1.14 of the MCF5249 User's Manual).

2.2 RAM Version

1. Fit the Biometrics Security daughter card to the M5249C3 EVB using the expansion connectors. The connectors are keyed and will only fit one way, with the sensor on the IDE connector side of the EVB and the LCD on the BDM connector side.
2. Ensure that jumper 12 is set to pins 1–2 to allow dBUG to boot.
3. Connect the RS232 cable from an available COM port on the PC to the terminal connector on the EVB.
4. Connect the Ethernet cable to the Ethernet connector on the EVB. If a network point is not available, it is possible to establish a direct connection to the PC with a crossed cable.
5. Set up Hyperterminal or another terminal emulation program on the PC as described in Section 2.1 of the M5249C3 User's Manual.
6. Set up the dBUG network parameters as described in Appendix A of the M5249C3 User's Manual. If a network point is not available and a direct connection is being used, set up the dBUG parameters to match the settings of the PC.
7. Ensure that the 5249BIO.bin binary image file is in the directory that the tftp server is currently monitoring.
8. Download the image file using the dBUG DN command (The image could also be downloaded using the dBUG DL command; however, using the DL command may take a long time).

3 Running the Application

The Flash and RAM versions of the application operate identically except that the Flash version will run immediately after the power is connected to the board assuming that jumper 12 is set to pins 2–3.

To run the application after it has been downloaded, type the following command at the dBUG prompt:

```
dBUG> go 20000
```

The terminal window will display the initialization of uClinux and the fingerprint application will run. The LCD will show a startup welcome message before going into fingerprint acquisition.

At startup, the application runs a calibration routine that adjusts the finger detection sequence to ambient sensor readings. During this routine, the LCD displays the following message, asking the user to refrain from touching the sensor until the calibration is complete:

*Sensor calibration:
Please dont touch*

The application has two modes, enrollment and verification, selected via the switch on the daughtercard. If the switch is set to verification when the application is run, verification begins and the application asks for a finger to be placed on the sensor. However, since this is the start of the demonstration, there is no template to which the fingerprint can be compared; therefore, verification will fail. Set the switch to enrollment, and place a finger on the sensor to reset the software to enrollment mode.

3.1 Enrollment Mode

In enrollment mode, the application runs the fingerprint acquisition and algorithm between four and seven times in order to create a template for future verification. The LCD displays the following message for each of the runs:

*Enroll: Score(0) = --
please re-place finger*

If a finger is not placed on the sensor, a timeout occurs, the enrollment fails, and the LCD displays the timeout message below. The application then returns to the start of the enrollment sequence.

*Enroll: Score(1) = --
Enrollment failed!..
(timeout reached)*

Upon completion of four or more successful fingerprint acquisitions, the enroll score shows an actual value, as in the example below. This value changes based on the clarity of the image, the number of minutia available for extraction, and the weight each minutia has been given according to prior matches. Though it is possible to keep the finger on the sensor throughout the seven acquisitions, to increase template quality, the finger should be lifted and replaced between each acquisition.

*Enroll: Score(4) = 41%
enrollment SUCCESFULL!..
switch to verification*

Completing seven acquisitions is more likely to produce a higher score because, with each additional acquisition, specific minutia can gain a higher weighting.

*Enroll: Score(7) = 77%
enrollment SUCCESFULL!..
switch to verification*

To stop the enrollment process, do not touch the sensor until a timeout has occurred. The LCD will display the final enroll score and will ask for the switch to be moved to verification. If the final score is less than 25%, then enrollment is insufficient and the process will be restarted as in the example below.

*Enroll: Score(5) = 22%
enrollment failed!..
(Score < 25%)*

NOTE

The demonstration will only store one fingerprint template at a time.

3.2 Verification Mode

In verification mode, the user's fingerprint is captured and compared against the template created during enrollment. After enrollment has been completed and the switch is set to verification, the LCD displays a message asking for a finger to be placed on the sensor. If no finger is placed, a timeout occurs and the LCD displays the same request. If a finger is placed on the sensor, the fingerprint will be captured and compared to the template.

If the fingerprint matches the template, then the following message will be displayed:

*Congratulations!
Your fingerprint has
been verified.*

If the fingerprint does not match the template, the following message will be displayed:

*Sorry,
Your fingerprint has
failed verification.*

The demonstration remains in verification mode until the switch is moved back to enrollment. When enrollment is selected, the previous template is erased and a new one is created by the next successful enrollment.

4 Additional Information

To demonstrate the versatility of the fingerprint algorithm during verification, the correct finger can be placed on the sensor in different orientations, or it can be moved around with a fixed orientation. Also, a comparison can be made between dry and wet fingers, resulting in different enroll scores. Experiments like these highlight how the correct fingerprint can be verified in a variety of conditions.

Another feature of the fingerprint algorithm can be used to alert the user to the verification of latent fingerprint images (residual fingerprints left on the surface of the sensor). Since these images can be used to fool the system if the sensor takes an image when no finger is present, the algorithm detects, based on adjustable rotational and translation thresholds, images that are too close or identical to the last matched fingerprint. If the captured fingerprint image is detected as identical to the previous matched image, the LCD will display a message that indicates this condition. The algorithm's ability to detect latent fingerprint images can be demonstrated during verification by leaving the finger on the sensor.

There is also a web server running on the MCF5249 as part of the application that displays the images taken from the sensor. There is one page that shows the seven images taken as part of the enrollment mode, and another page that shows the last image taken by the sensor.

To demonstrate the web server, connect a crossed Ethernet cable directly to the PC, and switch the proxy server off in Internet Explorer (Tools/Internet Options/Connections/LAN settings) before opening the webpage <http://10.0.0.10> via the address bar.

To return to booting with dBUG after using the Flash version, switch jumper 12 back to pins 1–2.

5 Revision History

Table 1 provides revision history information for this document.

Table 1. Revision History

Rev. No.	Substantial Changes	Date
0	Initial Release	December 2002
1	<ul style="list-style-type: none"> Section 3: added information about calibration routine. Section 4: added information about detection of latent fingerprint images. 	January 2003
2	<ul style="list-style-type: none"> Added Section 2.1, "Flash Version." Added web server information to Section 4. 	May 2003